



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/904,517	07/16/2001	Jian Kang Wu	24696	2272
7590	02/09/2005		EXAMINER	
			TESLOVICH, TAMARA	
			ART UNIT	PAPER NUMBER
			2137	

DATE MAILED: 02/09/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/904,517	WU ET AL.
	Examiner Tamara Teslovich	Art Unit 2137

— The MAILING DATE of this communication appears on the cover sheet with the correspondence address —

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) Responsive to communication(s) filed on 16 July 2001.

2a) This action is FINAL. 2b) This action is non-final.

3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) Claim(s) 48-85 is/are pending in the application.
4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) Claim(s) _____ is/are allowed.

6) Claim(s) 48-85 is/are rejected.

7) Claim(s) _____ is/are objected to.

8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) The specification is objected to by the Examiner.

10) The drawing(s) filed on 16 July 2001 is/are: a) accepted or b) objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) Notice of References Cited (PTO-892)
2) Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 6/28/02 9/05/01, 6/28/02 *(AV)*

4) Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____ .
5) Notice of Informal Patent Application (PTO-152)
6) Other: ____ .

DETAILED ACTION

Claims 1-47 have been cancelled by applicant.

Claims 48-85 are currently pending in application.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 48-85 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. Patent 5,606,609, hereinafter referred to as Houser et al.

As per claim 48, Houser et al. discloses a method for a person to sign a hard copy or a digital document by use of a signature sensing device, including the steps of:

- a) capturing a capturable signature of the person using the sensing device (see column 10 lines 38-51);
- b) generating a verification ID (see column 7 lines 29-44); and
- c) attaching the capturable signature, the verification ID, and an optical watermark to the document to complete the document signing process, characterized in that the capturable signature is embedded into the optical watermark, and the verification ID is generated from one or more of the group

consisting of: the capturable signature, a document digest, representative features of the document, and a time stamp (see column 8 lines 34-39 and column 8 lines 20-32).

As per claim 49, Houser et al. discloses a method as claimed in claims 48, characterized in that one or more selected from a group consisting of: the document digest and a time stamp is embedded into the optical watermark to form a link between the document and the capturable signature; the document digest being critical information of the document (see column 7 lines 44-60).

As per claim 50, Houser et al. discloses a method as claimed in claim 48, characterized in that a person's identity is verified by a public key infrastructure after a security handshaking challenge-and-response session between a server and the sensing device; the sensing device storing one or more selected from the group consisting of: an identity number of the sensing device, a private key of the sensing device, a private key of the person, measured features of the person's capturable signature, and a detachable learning module (see column 7 lines 66-67, column 8 lines 1-19, and column 9 lines 21-35).

As per claim 51, Houser et al. discloses a method as claimed in claim 50, characterized in that there is a plurality of persons able to use the sensing device, the sensing device being able to store registration information of each such person (see column 8 lines 1-19).

As per claim 52, Houser et al. discloses a method as claimed in claim 51, characterized in that the server and sensing device store their private keys respectively, and the capturable signature and/or measures features of the

capturable signature of the person are stored in the server; there being included a preliminary step of security handshaking between the server and the sensing device based on public key pairs (see column 7 lines 66-67, column 8 lines 1-19, and column 9 lines 36-67).

As per claim 53, Houser et al. discloses a method as claimed in claim 52, characterized in that the capturable signature and/or measures features of the capturable signature of the person are stored in the sensing device, and the processing and verification of the capturable signature are also carried out inside the sensing device (see column 7 lines 66-67, column 8 lines 1-19, and column 9 lines 1-19 and 36-67).

As per claim 54, Houser et al. discloses the method as claimed in claim 53, characterized in that there is a security authentication process between the server and the sensing device, as well as between the server and a service program; and after successful completion of the security handshaking, the sensing device collects capturable signature data, encrypts the capturable signature data, and sends it to the server for further processing and verification (see column 9 lines 1-35).

As per claim 55, Houser et al. discloses a method as claimed in claim 54, characterized in that the capturing and processing of the capturable signature and/or measured features of the capturable signature of the person are carried out in a secure processor; the processor result being sent to the sensing device for verification (see column 8 lines 50-65).

As per claim 56, Houser et al. discloses a method as claimed in claim 55, characterized in that the private key and the capturable signature of the person are stored in the sensing device (see column 9 lines 1-35).

As per claim 57, Houser et al. discloses a method as claimed in claim 55 characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in the secure processor (see column 8 lines 50-65 and column 14 lines 37-51).

As per claim 58, Houser et al. discloses a method as claimed in claim 55, characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in the server (see column 8 lines 50-65).

As per claim 59, Houser et al. discloses a method as claimed in claim 55, characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in encrypted form (see column 9 lines 61-67 and column 14 lines 37-51).

As per claim 60, Houser et al. discloses a method as claimed in claim 55, characterized in that the capturable signature and/or the measured features of the capturable signature of the person are stored in a secure memory (see column 9 lines 1-35 and column 14 lines 37-51).

As per claim 61, Houser et al. discloses a method as claimed in claim 60, characterized in that the secure memory is an authentication card for the person (see column 9 lines 21-60).

As per claim 62, Houser et al. discloses a method as claimed in claim 55, further including a document-handling module in the computer for displaying the document and incorporation of the capturable signature into the document (see column 8 lines 13-19).

As per claim 63, Houser et al. discloses a method as claimed in claim 62, further including at least one image in the sensing device so that upon signing the document both the capturable signature of the person and the at least one seal image will appear on the document (see column 8 lines 13-19).

As per claim 64, Houser et al. discloses a method as claimed in claim 63, characterized in that the at least one seal image is the optical watermark in which is embedded hidden information to protect against forgeries (see column 8 lines 20-32).

As per claim 65, Houser et al. discloses a method as claimed in claim 64, characterized in that the method is applied to process approval (see column 7 lines 15-28).

As per claim 66, Houser et al. discloses a method for generating a validated capturable signature to a document including the steps of:

- a) signing a document using signature sensing device (see column 8 lines 34-39);
- b) creating a digest of the document (see column 7 lines 44-60);
- c) encrypting the capturable signature with the sensing device (see column 9 lines 36-67);
- d) generating a verification ID (see column 7 lines 29-44); and

c) attaching the capturable signature and the verification ID and an optical watermark to the document to complete the document signing process, characterized in that one or more selected from the group consisting of the: the capturable signature, the document digest, and critical features of the document, are embedded into the optical watermark to form a link between the document and capturable signature (see column 8 lines 20-32).

As per claim 67, Houser et al. discloses a method as claimed in claim 66, characterized in that the verification ID is generated from one or more of the group consisting of: the capturable signature, the document digest, representative features of the document, and time stamp (see column 7 lines 44-60).

As per claim 68, Houser et al. discloses a method as claimed in claim 67, characterized in that the capturable signature and the time stamp are encrypted using an encryption key, the encryption key being generated from the document digest (see column 9 lines 37-67).

As per claim 69, Houser et al. discloses a method as claimed in claim 68, characterized in that the encryption key is generated by using the document digest to query an encryption key pair from an encryption key database in one of: the sensing device, a server, or a secure memory (see column 3 lines 61-67, column 4 lines 1-2, and column 5 lines 3-13 and 31-48).

As per claim 70, Houser et al. discloses a method as claimed in claim 68, characterized in that the encryption key is generated by using the document digest as a seed to generate an encryption key pair inside one selected from the

group consisting of: the sensing device, a server, and a secure memory, and using a secret function stored in one of: the sensing device, the server, and the secure memory (see column 3 lines 61-67, column 4 lines 1-2, and column 5 lines 3-13 and 31-48).

As per claim 71, Houser et al. discloses a method as claimed in claim 68, characterized in that the digest of the document is obtained from the representative features of the document (see column 7 lines 44-60).

As per claim 72, Houser et al. discloses a method as claimed in claim 71, characterized in that the capturable signature is extracted from a printed form of the document when the document to be verified is a printed document (see column 10 lines 38-51).

As per claim 73, Houser et al. discloses a method as claimed in claim 68, characterized in that the encryption key is one of a public key and a symmetry key (see column 9 lines 37-67).

As per claim 74, Houser et al. discloses a method as claimed in claim 64, characterized in that the capturable signature includes signature image and features of the capturable signature when features of the capturable signature are captured; the features of the capturable signature captured including pressure and speed (see column 10 lines 17-60).

As per claim 75, Houser et al. discloses a method as claimed in claim 71, characterized in that the capturable signature includes signature image and features of the capturable signature when features of the capturable signature

are captured; the features of the capturable signature captured including pressure and speed (see column 10 lines 17-60).

As per claim 76, Houser et al. discloses a method as claimed in claim 50, characterized in that pre-registered capturable signatures are stored for future use in one or more selected from the group consisting of: the sensing device, the server, and a secure memory (see column 10 lines 23-51 and Figure 4B).

As per claim 77, Houser et al. discloses a method as claimed in claim 68, characterized in that pre-registered capturable signatures are stored for future use in one or more selected from the group consisting of: the sensing device, the server, and a secure memory (see column 10 lines 23-51 and Figure 4B).

As per claim 78, Houser et al. discloses a method as claimed in claim 64, characterized in that the capturable signature is combined with other biometric information of the person (see column 12 lines 55-67, column 13 lines 1-20, column 16 lines 65-67, and column 17 lines 1-4).

As per claim 79, Houser et al. discloses a method as claimed in claim 72, characterized in that the capturable signature is combined with other biometric information of the person (see column 12 lines 55-67, column 13 lines 1-20, column 16 lines 65-67, and column 17 lines 1-4).

As per claim 80, Houser et al. discloses a method as claimed in claim 64, characterized in that the authenticity of the signed document is verified by:

- a) creating a digest of the signed document (see column 7 lines 44-60);

Art Unit: 2137

- b) querying or generating a decrypt key using the document digest, and decrypting the verification ID (see column 5 lines 3-13 and lines 31-48 and column 16 lines 10-23) ; and
- c) verifying the validity of the capturable signature by comparing the capturable signature extracted from the verification ID and the capturable signature as it appears on the signed document (see column 3 lines 61-67, column 4 lines 1-2, column 5 lines 31-48, and column 16 lines 10-23).

As per claim 81, Houser et al. discloses a method as claimed in claim 72, characterized in that the authenticity of the signed document is verified by:

- a) creating a digest of the signed document (see column 7 lines 44-60);
- b) querying or generating a decrypt key using the document digest, and decrypting the verification ID (see column 5 lines 3-13 and lines 31-48 and column 16 lines 10-23); and
- c) verifying the validity of the capturable signature by comparing the capturable signature extracted from the verification ID and the capturable signature as it appears on the signed document (see column 3 lines 61-67, column 4 lines 1-2, column 5 lines 31-48, and column 16 lines 10-23).

As per claim 82, Houser et al. discloses a method as claimed in claim 80, characterized in that there is included the additional step of verifying the authenticity of the document by comparing the document digest and a digest from the verification ID (see column 3 lines 61-67 and column 4 lines 1-2).

As per claim 83, Houser et al. discloses a method as claimed in claim 81, characterized in that there is included the additional step of verifying the

Art Unit: 2137

authenticity of the document by comparing the document digest and a digest from the verification ID (see column 3 lines 61-67 and column 4 lines 1-2).

As per claim 84, Houser et al. discloses a method as claimed in claim 82, characterized in that there is included the further step of verifying the authenticity of the document by comparing the capturable signature on the document and critical features of the document with that embedded in the optical watermark (see column 3 lines 61-67 and column 4 lines 1-2).

As per claim 85, Houser et al. discloses a method as claimed in claim 83, characterized in that there is included the further step of verifying the authenticity of the document by comparing the capturable signature on the document and critical features of the document with that embedded in the optical watermark (see column 3 lines 61-67 and column 4 lines 1-2).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tamara Teslovich whose telephone number is (571) 272-4241. The examiner can normally be reached on Mon-Fri 8-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



**ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER**